

EXHIBIT C-1



Source: https://store.google.com/us/product/pixel_4a?hl=en-US

Processors

Qualcomm® Snapdragon™ 730G⁴

Source: https://store.google.com/us/product/pixel_4a_specs?hl=en-US

FIG. 1

Device security

- **Screen lock**
Lock your phone with a PIN, pattern, or password. Learn how to set a screen lock.
- **Lock screen preferences**
Choose which notifications show when your screen is locked. Learn how to control notifications..
- **Lockdown**
Turn off notifications, fingerprint or face recognition unlocking, and Smart Lock while on your lock screen. Learn how to turn on lockdown.
- **Emergency information**
Add text to your lock screen, like info to help someone return your phone if you lost it. Learn how to put a message on your lock screen.
- **Pixel Imprint**
Use your fingerprint to unlock your phone and authorize purchases. Learn how to set up fingerprints.
- **Smart Lock**
Set your device to stay unlocked in certain circumstances. Learn how to turn on Smart Lock.

Source: <https://support.google.com/pixelphone/answer/2824802?hl=en>

Memory and Storage

6 GB LPDDR4x RAM • 128 GB storage³

Source: https://store.google.com/us/product/pixel_4a_specs?hl=en-US

FIG. 2

1. From a Home screen, swipe up to display all apps.
2. Navigate: **Settings** ⓘ > **Security** > **Screen lock**.
→ If prompted to add a Google account:
 - Tap Add Google account now to set up an account.
 - Tap **Continue** to proceed without setting up an account.
→ If presented, enter the current PIN, password or pattern.
3. Do one of the following:
 - Set up a screen lock:
 - Pattern
 - PIN
 - Password
 - Disable screen lock:
 - a. Tap 'None' or 'Swipe'.
 - b. To confirm, tap **Yes, remove**.

Source: <https://www.verizon.com/support/knowledge-base-228614/>

FIG. 3

Pattern

 An unlock pattern is created to access the device.

1. Tap **Pattern**.
2. Draw an unlock pattern (connecting at least 4 dots) then tap **Next**.
3. Draw the same pattern again then tap **Confirm**.
4. If prompted, tap one of the following then tap **OK**:
 - Show all notifications
 - Hide sensitive notification content
 - Hide all notifications

Source: <https://www.verizon.com/support/knowledge-base-228614/>

FIG. 4

Set up your first fingerprint

1. Open your phone's Settings app.
2. Tap **Security**.
3. Tap **Pixel Imprint**.
4. Follow the on-screen steps. If you don't already have a screen lock, you'll be asked to add a backup PIN, pattern, or password.
5. Scan your first fingerprint. Tips:
 - Put your finger on your phone's sensor (not its screen).
 - Hold your phone as you'd normally hold it when unlocking. For example, hold your phone with its screen facing you.

<https://support.google.com/pixelphone/answer/6285273#zippy=%2Cset-up-your-first-fingerprint%2Cremove-rename-or-replace-your-fingerprints>

Sensors

Proximity / Ambient light sensor

Accelerometer / Gyrometer

Magnetometer

Pixel Imprint™ – back-mounted fingerprint sensor for fast unlocking

Barometer

Android Sensor Hub

Source: https://store.google.com/us/product/pixel_4a_specs?hl=en-US

FIG. 5

1. From a Home screen, swipe up to display all apps.
2. Navigate: **Settings** ⓘ > **Security** > **Screen lock**.
→ If prompted to add a Google account:
 - Tap Add Google account now to set up an account.
 - Tap **Continue** to proceed without setting up an account.
→ If presented, enter the current PIN, password or pattern.
3. Do one of the following:
 - Set up a screen lock:
 - Pattern
 - PIN
 - Password
 - Disable screen lock:
 - a. Tap 'None' or 'Swipe'.
 - b. To confirm, tap **Yes, remove**.

Source: <https://www.verizon.com/support/knowledge-base-228614/>

Pattern

 An unlock pattern is created to access the device.

1. Tap **Pattern**.
2. Draw an unlock pattern (connecting at least 4 dots) then tap **Next**.
3. Draw the same pattern again then tap **Confirm**.
4. If prompted, tap one of the following then tap **OK**:
 - Show all notifications
 - Hide sensitive notification content
 - Hide all notifications

Source: <https://www.verizon.com/support/knowledge-base-228614/>

FIG. 6

Set up your first fingerprint

1. Open your phone's Settings app.
2. Tap **Security**.
3. Tap **Pixel Imprint**.
4. Follow the on-screen steps. If you don't already have a screen lock, you'll be asked to add a backup PIN, pattern, or password.
5. Scan your first fingerprint. Tips:
 - Put your finger on your phone's sensor (not its screen).
 - Hold your phone as you'd normally hold it when unlocking. For example, hold your phone with its screen facing you.

<https://support.google.com/pixelphone/answer/6285273#zippy=%2Cset-up-your-first-fingerprint%2Cremove-rename-or-replace-your-fingerprints>

Memory and Storage

6 GB LPDDR4x RAM • 128 GB storage³

Source: https://store.google.com/us/product/pixel_4a_specs?hl=en-US

FIG. 7

Pattern

 An unlock pattern is created to access the device.

1. Tap **Pattern**.
2. Draw an unlock pattern (connecting at least 4 dots) then tap **Next**.
3. Draw the same pattern again then tap **Confirm**.
4. If prompted, tap one of the following then tap **OK**:
 - Show all notifications
 - Hide sensitive notification content
 - Hide all notifications

Source: <https://www.verizon.com/support/knowledge-base-228614/>

Set up your first fingerprint

1. Open your phone's Settings app.
2. Tap **Security**.
3. Tap **Pixel Imprint**.
4. Follow the on-screen steps. If you don't already have a screen lock, you'll be asked to add a backup PIN, pattern, or password.
5. Scan your first fingerprint. Tips:
 - Put your finger on your phone's sensor (not its screen).
 - Hold your phone as you'd normally hold it when unlocking. For example, hold your phone with its screen facing you.

<https://support.google.com/pixelphone/answer/6285273#zippy=%2Cset-up-your-first-fingerprint%2Cremove-rename-or-replace-your-fingerprints>

Memory and Storage

6 GB LPDDR4x RAM • 128 GB storage³

Source: https://store.google.com/us/product/pixel_4a_specs?hl=en-US

FIG. 8

We strongly recommend locking your screen to help protect your phone. Your fingerprint sensor gives you a convenient unlocking option.

But there are a few things to keep in mind:

- A fingerprint can be less secure than a strong PIN, pattern, or password.
- A copy of your fingerprint could be used to unlock your phone. You leave fingerprints on many things you touch, including your phone.
- You'll be asked to add a backup PIN, pattern, or password. Remember your backup, because you'll need to use it sometimes, like after restarting your phone, or if your fingerprint isn't recognized.

Where your fingerprint data is stored


Your fingerprint data is stored securely and never leaves your phone. Your data is not shared with Google or apps on your phone. Learn more about how fingerprint data is secured.

Source: <https://support.google.com/pixelphone/answer/6285273#zippy=%2Cabout-fingerprint-security>

FIG. 9

Setting the Supervisor Password/User Password

Set the Supervisor Password before setting the User Password.

1. Start up the Setup Utility. ( **Starting the Setup Utility**)
2. Touch [Security] menu.
3. Double-touch [Set Supervisor Password] or [Set User Password].
4. Enter your password in [Create New Password] and touch <Enter>.
 - When the password has been set, you need to enter your password in [Enter Current Password] and touch <Enter>.
 - To disable the password, leave the input field empty and touch <Enter>.
5. Enter your password again in [Confirm New Password] and touch <Enter>.
6. Touch <F10>, and then select [Yes] and touch <Enter>.
 - When using the on-screen keyboard <F10> key, touch [SYM] - [F10].

Source: https://na.panasonic.com/ns/272159_TOUGHPAD_FZ-G1_Reference_Manual.pdf (Pg. 59)

How it works

The Windows Hello face recognition engine consists of four distinct steps that allow Windows to understand who is in front of the sensor:

1. Find the face and discover landmarks

In this first step, the algorithm detects the user's face in the camera stream and then locates facial landmark points (also known as alignment points), which correspond to eyes, nose, mouth, and so on.

2. Head orientation

To ensure the algorithm has enough of your face in view to make an authentication decision, it ensures the user is facing towards the device +/- 15 degrees.

3. Representation vector

Using the landmark locations as anchor points, the algorithm takes thousands of samples from different areas of the face to build a representation. The representation at its most basic form is a histogram representing the light and dark differences around specific points. No image of the face is ever stored – it is only the representation.

4. Decision engine

Once there is a representation of the user in front of the sensor, it is compared to the enrolled users on the physical device. The representation must cross a machine-learned threshold before the algorithm will accept it as a correct match. If there are multiple users enrolled on the system, this threshold will increase accordingly to help ensure that security is not compromised.

Source: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication>

FIG. 8